WHITEPAPER

Matillion security whitepaper

matillion

Table of contents

Table of contents

Matillion's Approach to Security: Comprehensive and Collaborative

In Matillion, we see security as a shared task that reaches beyond just one team. It is an integral part of every aspect of our operations, from product development to day-to-day business operations to IT infrastructure. A strong and reliable security framework is a fundamental part of everything we do.

This whitepaper introduces our security program and product architecture, providing a clear and accessible overview of our commitment to enterprise-level security.

The whitepaper also describes how we focus on maintaining customer trust through our rigorous security protocols and provide a clear understanding of our proactive approach to security, which meets or exceeds industry standards as reflected in every part of the Matillion Security Framework.

Security by Design

Security by design represents a foundational approach that seamlessly integrates security measures and considerations into the very fabric of systems, products, and processes right from their inception. This proactive methodology prioritizes the early identification and mitigation of potential security risks, rather than relying solely on reactive measures after vulnerabilities have been exposed. By incorporating security as an inherent part of the design process, Matillion fosters the creation of robust and resilient systems that possess the capability to effectively withstand and deter cyber threats.

Security by design encompasses a holistic perspective, encompassing not only technical aspects but also critical factors such as user behavior, access controls, and data privacy. By adopting this comprehensive mindset, we establish a solid foundation for enhanced security, ensuring that it permeates every layer of their infrastructure and operations. This approach empowers Matillion to proactively address potential security challenges, building a resilient framework that safeguards against evolving threats and instills confidence in the protection of valuable assets and sensitive information.

Compliance and Certification

Compliance and certification play a crucial role in protecting sensitive information. Certifications provide an objective assessment of our security practices, validating our commitment to upholding the highest standards of data protection. By subjecting ourselves to rigorous audits and assessments, we ensure that our security measures align with industry standards and best practices.

Recognizing the dynamic nature of the security landscape, we understand the importance of continuous improvement. Compliance standards necessitate regular reviews and updates to ensure ongoing adherence to industry fundamentals. By embracing these standards, we reinforce our commitment to maintaining the utmost level of security.

Matillion certification reports serve as tangible evidence of the stringent security measures we implement across our organization. These reports are publicly available, underscoring our transparency and commitment to providing comprehensive security information. To access customer security artifacts, please visit matillion.com/trust-center where customers can securely download the necessary documentation.

- SOC1 TYPE2, SOC2 TYPE2, and SOC3
- ISO 27001
- Cloud Security Alliance (CSA), Security, Trust, Assurance and Risk Registry (STAR) Level One registered
- PCI DSS — Matillion has completed the SAQ-D self attestation as a merchant(Report can be downloaded from our Trust Center)
- HIPAA (BAA available)
- GDPR / CCPA compliance
- NIST Cybersecurity Framework standards
- OWASP and SAMM development and assurance practices

Matillion Security Organization

Under the leadership of the Chief Information Security Officer (CISO), Matillion's Security Organization encompasses distinct areas of expertise to ensure comprehensive protection. The following departments coordinate to address all aspects of Matillion's security policy:

Governance, Risk, and Compliance: This department focuses on establishing robust security governance frameworks, assessing risks, and ensuring compliance with relevant regulations and industry standards. They play a pivotal role in defining security policies, conducting risk assessments, and overseeing compliance efforts to safeguard Matillion and our customers' sensitive information.

Application Security: The Chief Engineering Officer co-sponsors Matillion's adherence to industry-standard processes in our software applications throughout their development and deployment lifecycle. They employ industry best practices to identify and mitigate potential vulnerabilities, conduct rigorous security testing, and ensure secure coding practices are adhered to. By proactively addressing application-level risks, this team helps fortify our products against potential threats.

Security Operations: The Security Operations team is dedicated to continuous monitoring, incident response, implementation of security controls, and threat detection across Matillion's infrastructure. They act as subject matter experts in prompt identification and mitigation of security incidents and in managing the end to end incident response efforts.. This team minimizes potential impact and strengthens our overall security posture through a proactive security posture and swift incident resolution.

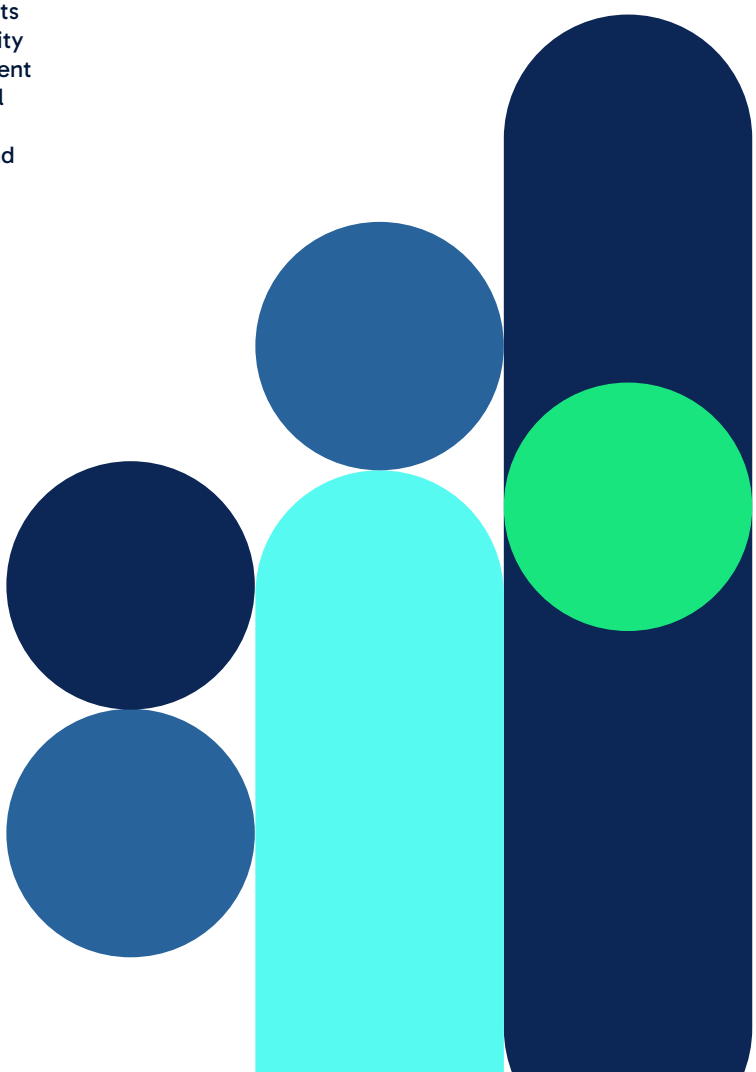
This structured approach enables specialized teams to address security concerns with precision, agility, and efficiency. These dedicated departments ensure Matillion can respond rapidly to various types of security issues, providing timely resolutions and enhancing our overall security capabilities.

The collective efforts of these departments ensure that Matillion's Security Organization holds security as a top priority throughout our operations, products, and services, empowering us to deliver a secure and trustworthy experience to our valued customers.

Risk Management

Matillion adopts internationally recognised frameworks, such as ISO 27005 and NIST as the basis for its risk management and assessment practices. Through adherence to these established frameworks, we ensure a systematic and comprehensive approach to managing information risk throughout our organization.

Leveraging ISO 27005, NIST, and our robust Information Security Governance framework, Matillion maintains a diligent and structured approach to risk management. Our commitment to these processes enables us to proactively identify, assess, and address information security risks, thereby safeguarding our organization and the valuable assets entrusted to us.



Vulnerability Management

Matillion places a strong emphasis on maintaining a robust vulnerability management program to proactively identify and address vulnerabilities within our virtual infrastructure and customer-facing products. Our approach encompasses a variety of effective measures to ensure comprehensive vulnerability scanning, categorization, and timely remediation in accordance with our internal policies and established cadences.

For our virtual infrastructure, we employ cloud-native vulnerability scanning platforms to scan and assess the security posture of our infrastructure components. This enables us to identify vulnerabilities and prioritize their severity for prompt patching and mitigation.

In the case of our applications, we implement continuous scanning using advanced Software Composition Analysis

(SCA) tools, as well as Static and Dynamic Application Security Testing (SAST and DAST) tooling. These scanning methods are seamlessly integrated into our development pipelines, allowing for ongoing identification and resolution of vulnerabilities throughout the software development lifecycle.

To further ensure the robustness of our security measures, Matillion conducts routine third-party penetration testing. This comprehensive testing covers the entire web application surface area, providing valuable insights into potential vulnerabilities and helping us fortify our defenses.

In our commitment to transparency and collaboration, we actively encourage customer and community engagement. Matillion maintains a responsible disclosure pathway, enabling product users to report vulnerabilities they may discover, which we promptly address.

Additionally, we run a bug bounty platform to incentivize security researchers to scrutinize our systems and report any potential security issues they uncover. This program not only bolsters our vulnerability identification efforts but also fosters a mutually beneficial partnership with the security research community.

These comprehensive vulnerability management practices ensure that potential vulnerabilities are diligently identified, assessed, and addressed.

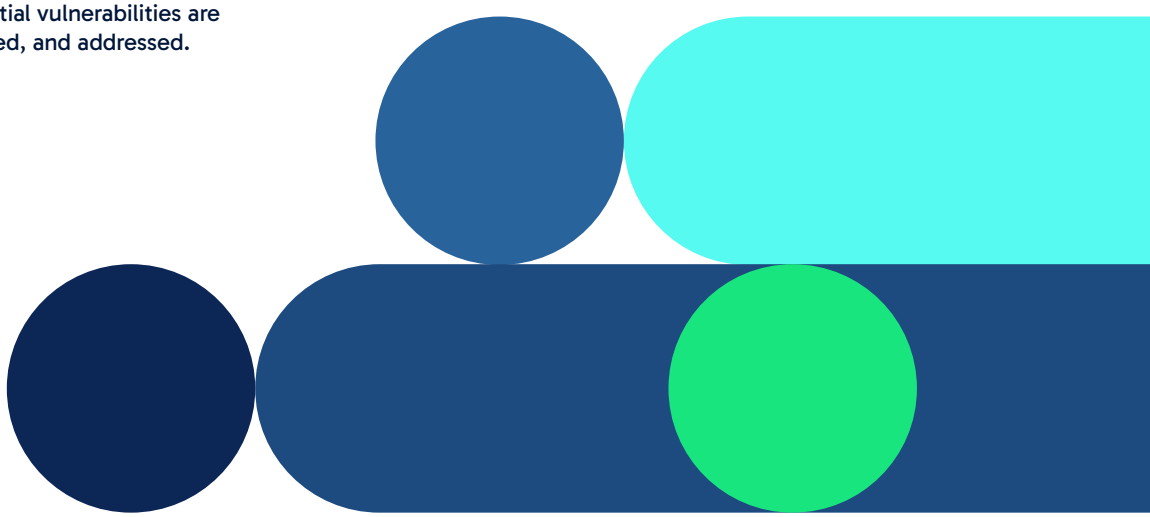
Third-Party Vendors

At Matillion, we recognize the value and importance of third-party platforms in delivering our products and services. To maintain the integrity of our security ecosystem, we have implemented a comprehensive approach to managing third-party vendors. Each vendor is carefully categorized based on their level of access to internal data or their significance within the Matillion ecosystem and service proposition.

To ensure the highest standards of security, all vendors undergo a thorough security review during the onboarding process. This review assesses their security practices, controls, and compliance with relevant standards and regulations, establishing a strong foundation of trust and accountability with our vendors from the outset.

Moreover, we believe in the importance of ongoing oversight and monitoring. Through our vendor risk management program, we conduct regular security reviews of our vendors throughout their lifecycle, ensuring that they continue to meet our stringent security standards and maintain a proactive approach to security.

Matillion implements these measures to ensure that our third-party vendors align with our commitment to maintaining a robust and secure environment. This approach enables us to mitigate potential security risks associated with third-party interactions and reinforces our dedication to safeguarding the confidentiality, integrity, and availability of our customers' data and our services as a whole.



Internal Identity and Access

Matillion Data Productivity Cloud prioritizes secure internal identity and access management to maintain strict control over authentication and authorization processes for all internal applications. To achieve this, we employ both Single Sign-On (SSO) and Multi-Factor Authentication approaches, ensuring centralized control and management of user authentication across our systems.

Our identity and access management strategy adheres to the principle of least privilege and role-based access. This ensures that users are granted access only to the applications and information that they are authorized to access based on their specific roles and responsibilities within the organization. Implementing these principles ensures we minimize the risk of unauthorized access and data breaches.

To bolster the effectiveness of our identity and access management measures, we leverage best-of-breed technologies. These technologies are carefully selected to provide robust security, seamless user experiences, and extensive auditing capabilities. This allows us to monitor and track access activities, maintaining a comprehensive audit trail for compliance and security purposes.

Matillion adopts these measures to ensure that internal identity and access management remain a top priority. We provide our users with secure and convenient access to the applications they need while implementing strict controls to protect sensitive information and prevent unauthorized access.

Disaster Recovery and Business Continuity

Matillion places significant emphasis on disaster recovery and business continuity to ensure resilience and uninterrupted operations in the face of unforeseen events. We have implemented a robust framework consisting of a comprehensive Disaster Recovery Plan (DRP) and a Business Continuity Plan (BCP).

Our DRP and BCP serve as essential guides, providing a structured approach to responding to and recovering from situations that may impact our business. These plans undergo regular review and testing on an annual basis to ensure their effectiveness and alignment with evolving business needs and potential threats.

To ensure widespread awareness and preparedness, our plans are readily accessible to all employees. Key roles within the organization receive comprehensive training on the plans, equipping them with the knowledge and skills necessary to execute their responsibilities effectively during critical situations.

The DRP comprises eleven run books, each tailored to address specific disaster scenarios. These run books outline predefined steps, actions, and procedures to be followed in response to different types of disasters, enabling a swift and organized recovery process. By covering a range of potential scenarios, we enhance our ability to handle various contingencies with efficiency and precision.

Matillion remains committed to maintaining a robust disaster recovery and business continuity framework, continuously striving to improve our response capabilities. Through ongoing review, testing, and training, we ensure that our plans remain up to date and that our teams are prepared to navigate unforeseen challenges. We prioritize these measures to safeguard our operations, protect our customers' interests, and reinforce our commitment to delivering uninterrupted services.

Matillion is hosted in the data centres managed by Amazon Web Services In the EU - Ireland is the main site, and Paris is the backup site. In the US - North Virginia is the main site, and Ohio is the backup site.

Incident Response

Matillion recognizes the critical importance of swift and effective incident response to ensure the security and integrity of our systems and data. We maintain a robust incident response plan designed to address security incidents promptly and efficiently, regardless of their priority.

Our incident response plan undergoes thorough testing on an annual basis to ensure the preparedness of our teams. We conduct tabletop exercises and fire drills, simulating various incident scenarios to assess our readiness and enhance our response capabilities. These exercises provide valuable practice and enable all functions within Matillion to respond quickly and effectively in the event of an incident.

In line with our commitment to continuous improvement, we have established a Post Incident Report (PIR) process. This process facilitates the documentation and analysis of security incidents, identifying lessons learned and actionable recommendations. Leveraging the insights gained from these reports, we can implement necessary enhancements to our systems, processes, and procedures, fortifying our defenses against future incidents.

In the event of a complex incident, Matillion has a contingency plan in place to access additional resources for incident response and forensics. This plan ensures that we can mobilize and utilize retained expertise to address the incident comprehensively and minimize its impact.

Maintaining a comprehensive incident response plan, conducting regular testing, and leveraging post-incident analysis, provides assurance that Matillion is well-prepared to handle security incidents swiftly and effectively. Our commitment to continuous improvement and resource allocation ensures that we can mitigate the effects of incidents, protect our systems and data, and provide a secure environment for our customers and stakeholders.

Physical Security

While Matillion operates primarily on cloud platforms, we recognize the importance of physical security measures to safeguard our office locations and any associated infrastructure. Although our reliance on physical infrastructure is limited due to the nature of our cloud-based operations, we have implemented a number of measures to ensure the physical security of our premises.

Our office locations are equipped with a secure overlay and manned receptions to regulate access and monitor visitors. This helps maintain a controlled environment and ensures that only authorized individuals can enter our facilities. Additionally, we implement card-based access control systems to further restrict entry to authorized personnel.

To enhance network security, we employ secure internet breakout networks that provide a protected connection to the internet, minimizing the risk of unauthorized access or malicious activities.

To provide an additional layer of security and surveillance, our office locations are equipped with CCTV coverage. This allows for continuous monitoring of our premises, providing visual records that can assist in investigating and addressing security incidents.

Furthermore, it is worth noting that all our infrastructure is hosted by industry-leading cloud infrastructure providers. These providers prioritize physical security within their data centers, implementing comprehensive measures to protect the underlying infrastructure that supports our operations.

Implementing these physical security measures ensures Matillion can protect our office locations, infrastructure, and any associated assets. We remain committed to maintaining a secure environment to safeguard our operations and the data entrusted to us.

Data Privacy

At Matillion, we prioritize data privacy as a fundamental aspect of our security program. We are fully committed to complying with all relevant data privacy regulations, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

To ensure the protection of personal data, we strictly adhere to the principle of processing only the minimum amount of personal data necessary for the performance of our contractual obligations with customers, legitimate interests pursued by us, and customer support functions. This approach allows us to minimize data exposure and maintain a high level of privacy.

We implement appropriate technical and organizational measures to safeguard personal data. These measures are designed to protect the confidentiality, integrity, and availability of the data we handle. By leveraging industry best practices and utilizing robust security controls, we ensure that personal data is adequately protected against unauthorized access, disclosure, alteration, or destruction.

We are committed to preventing any secondary use of personal data beyond the purposes outlined in our contracts or as required by law. Our systems are designed to securely store personal data in a third-party sales platform, where it is retained for no longer than necessary. This helps us ensure data minimization and responsible data management practices.

Matillion prioritizes the protection and privacy of personal data by adhering to data privacy regulations, implementing security measures, and adopting a data-centric approach. We understand the importance of maintaining the trust of our customers and are dedicated to handling personal data in a secure and responsible manner.

International Transfers

Matillion recognizes the importance of ensuring the security and protection of data when transferring it to third countries. We prioritize conducting transfer impact assessments to evaluate the potential risks associated with such transfers.

To ensure the appropriate safeguards are in place, we utilize a combination of measures, including but not limited to:

- **UK International Data Transfer Agreement (IDTA):** When transferring data to countries outside of the United Kingdom, we adhere to the requirements outlined in the UK IDTA. This agreement provides a framework for ensuring that data transfers meet the necessary legal and security standards.
- **UK Data Protection Act (DPA):** We comply with the provisions of the UK DPA when transferring data internationally. This legislation ensures that appropriate safeguards are implemented to protect the rights and privacy of individuals' personal data.
- **EU Standard Contractual Clauses (SCCs):** In cases where data is transferred to countries within the European Union or other countries recognized by the EU as providing an adequate level of data protection, we rely on the EU SCCs. These clauses establish contractual obligations between Matillion and the recipients of the data, ensuring that the transferred data remains protected.
- **EU Data Protection Authorities (DPAs):** We engage with EU DPAs to seek guidance and assistance in implementing appropriate safeguards for international data transfers. This collaboration helps us stay updated on the latest regulatory requirements and best practices to ensure the security of transferred data.

By employing these measures, Matillion ensures the security and protection of data when transferring it internationally and we are committed to complying with applicable laws and regulations and implementing safeguards that align with the highest standards of data protection and privacy.

Sub-Processors

At Matillion, we require all our processors and sub-processors to implement safeguards that are at least equivalent to the robust measures we have in place.

When engaging with processors and sub-processors, we ensure that they have a strong commitment to data protection and privacy. We conduct a thorough evaluation of their security practices, technical capabilities, and compliance with applicable regulations.

As part of our due diligence process, we verify that our processors and sub-processors have implemented safeguards that align with our own stringent requirements. These safeguards are designed to protect the confidentiality, integrity, and availability of the data they handle on our behalf.

Holding our processors and sub-processors to these high standards maintains a consistent level of data protection throughout our ecosystem. This approach helps us ensure that the personal data entrusted to us by our customers remains secure, regardless of whether it is processed by Matillion or by our trusted partners.

We maintain strong contractual agreements with our processors and sub-processors, which include specific provisions for data protection, security measures, and ongoing monitoring. These agreements outline the expectations and obligations regarding data protection, reinforcing our commitment to safeguarding the privacy of our customers' data.

Matillion works with processors and sub-processors who share our commitment to data protection and security; Enforcing stringent requirements and maintaining strong partnerships is central to our cohesive approach to data protection and ensuring that the data entrusted to us receives the highest level of care and security throughout its lifecycle. Matillion has established DPA (Data processing Agreement) to provide assurance on data protection measures between processor and controller. Sub-processors are listed at the bottom of the web page in our DPA.

Consent Management

Matillion values the importance of consent in the processing of personal data. If we rely on customer consent for processing data, and customers have the right to withdraw that consent at any time without facing any negative consequences.

When consent is withdrawn, we promptly stop any processing activities that were based on that consent. We make the process of withdrawing consent easy and provide clear instructions on how to do so.

However, it's important to note that in some cases, we may still be allowed to use customer data even after consent is withdrawn. This may happen if we have a legitimate reason for doing so, as permitted by applicable data protection laws. We carefully assess these reasons and ensure they align with customer rights and interests.

Data Subject Rights

Matillion is committed to respecting customer privacy rights and ensuring that data subject rights are protected. We have established a robust process to handle data subject rights requests promptly and effectively.

To keep customers informed about how personal data is processed, we regularly update our privacy notice. This notice provides clear and transparent information about the data we collect, how we use it, and rights regarding personal information.

We handle rights requests in a timely manner, acknowledging receipt of requests and providing a response within the legally required timeframe.

For more detailed information about how we process personal data, please visit our website at www.matillion.com/privacy. This resource provides comprehensive information on our data processing practices, including the purposes of processing, lawful bases, and personal data rights.

We value transparency, accountability, and the security of personal data, and we are committed to providing a positive experience when it comes to exercising personal data rights.

Security Practices

Security Awareness

Matillion prioritizes security awareness as a fundamental aspect of our company culture. We ensure that all our staff members are well-informed and equipped with the knowledge and skills to contribute to a secure working environment.

To achieve this, we provide comprehensive security awareness training to all employees during their business onboarding process. This initial training familiarizes them with our security policies, procedures, and best practices. It ensures that they understand the importance of data protection, privacy, and their role in maintaining a secure environment for our customers and the organization.

We recognize that cybersecurity threats and best practices evolve over time. Therefore, we also conduct annual security awareness training sessions to keep our employees up to date with the latest security trends, emerging threats, and mitigation strategies. These training sessions reinforce their understanding of security protocols and equip them with the knowledge to identify and respond to potential risks effectively.

In addition to training, we foster a culture of open communication and awareness regarding security events. We regularly distribute communications across the business to keep our employees informed about the latest security incidents, trends, and proactive measures they can take to protect themselves and our organization.

By consistently emphasizing security awareness, we empower our employees to be vigilant, responsible, and proactive in safeguarding sensitive information and mitigating security risks. This collective effort contributes to a strong security posture and enhances our ability to protect our customers' data.

Matillion believes that security is everyone's responsibility. Through ongoing training and communication, we ensure that all staff members understand the importance of security and are actively engaged in maintaining a secure environment for our customers and our organization.

Vulnerability Scanning

Proactive identification and mitigation of vulnerabilities across our assets is core to our software strategy. To achieve this, we conduct both internal and external vulnerability scanning and package monitoring. These activities enable us to assess and address potential security weaknesses in our systems.

To ensure compliance with separation of duties standards, our Security department collaborates with asset owners to configure and operate scanning tools effectively. This collaborative approach allows us to leverage the expertise of both teams and ensure comprehensive coverage in our vulnerability scanning efforts.

When vulnerabilities are identified, we employ industry-recognized standards such as the Common Vulnerability Scoring System (CVSS) and the Exploit Prediction Scoring System (EPSS) to determine their severity. The CVSS score, combined with the EPSS, captures the characteristics of the vulnerabilities and assigns a numerical value. This quantitative value is then translated into a priority level (critical, high, medium, low) to facilitate SLA tracking and prioritize remediation efforts.

By utilizing this standardized approach, we can effectively prioritize our response to identified vulnerabilities and allocate resources accordingly. Critical and high-priority vulnerabilities receive immediate attention to ensure swift remediation, while medium and low-priority vulnerabilities are addressed within defined timelines based on our SLAs.

Through our vulnerability scanning and prioritization process, we enhance the security posture of our systems and protect our assets from potential exploits. By systematically identifying and addressing vulnerabilities, we minimize the risk of security incidents and strengthen the overall resilience of our infrastructure.

Maintaining a robust vulnerability management program that aligns with industry best practices is critical to Matillion's security posture. Our proactive approach ensures that identified vulnerabilities are addressed promptly and in accordance with their severity, enabling us to safeguard our systems and protect the confidentiality, integrity, and availability of our data.

Secure Software Development

The implementation of secure software development practices to ensure the delivery of robust and resilient software solutions is a high priority for Matillion. Our approach revolves around a well-defined Secure Software Development Life Cycle (SSDLC) that adheres to industry standards, including the OWASP (Open Web Application Security Project) guidelines. This comprehensive process ensures that security considerations are integrated throughout the entire software development journey, from the initial design phase to the final product delivery.

Our SSDLC encompasses various activities and practices to build secure and reliable software solutions. While not exhaustive, some key components of our secure software development process include:

- **Non-Functional Security Requirements:** We identify and define non-functional security requirements at the outset of each software development project. These requirements serve as the foundation for incorporating security controls and mitigations throughout the development process.
- **Threat Modeling:** We conduct thorough threat modeling exercises to identify potential vulnerabilities and security risks specific to each software solution. Threat modeling occurs each time a service is introduced or significantly modified, allowing us to proactively implement appropriate security measures to mitigate risks.
- **Static Analysis Security Testing (SAST):** We employ static analysis tools to scan and analyze the source code of our software applications and their dependencies. This helps us identify potential security vulnerabilities and coding errors early in the development cycle, allowing for timely remediation.
- **Dynamic Analysis Security Testing (DAST):** We conduct dynamic analysis security testing to evaluate the security posture of our software applications in real time. By simulating various attack scenarios, we can identify vulnerabilities and assess the effectiveness of our security controls.
- **Software Composition Analysis (SCA):** We utilize software composition analysis tools to identify and assess the security of third-party software components and libraries used in our applications. This helps us identify and address any known vulnerabilities or weaknesses associated with these components.

Incorporating these practices into our software development process ensures that security is a foundational aspect of our solutions. We prioritize the identification and mitigation of potential security risks throughout the entire development lifecycle, enabling us to deliver software products that meet the highest security standards.

We continually enhance our secure software development practices to adapt to evolving threats and industry best practices. By considering security from the earliest design phases and employing industry-standard tools and techniques, we provide our customers with software solutions that are secure, reliable, and resilient against potential threats.

Matillion products

The Matillion product portfolio consists of a number of applications which provide comprehensive data management and integration capabilities. Matillion Data Productivity Cloud comprises Matillion's fully-managed and hybrid-cloud applications: Designer, Data Loader and Data Productivity Cloud Streaming, each offering unique capabilities in moving, transforming and orchestrating data. Matillion Data Productivity Cloud also includes Hub, which provides administration, usage tracking, observability, and authentication/authorization across the platform.

Lastly, Matillion ETL is a comprehensive VM-deployed data integration pipeline designer which resides in the customer network. Matillion ETL is integrated with Hub, enabling hybrid-cloud capabilities.

Matillion Data Productivity Cloud

Matillion Data Productivity Cloud is a hybrid cloud SaaS platform designed to empower customers in managing their data effectively. With this platform, users create data pipelines that support data movement, data transformation, and data orchestration. Furthermore, it offers robust admin and operational visibility to manage the entire platform end to end.

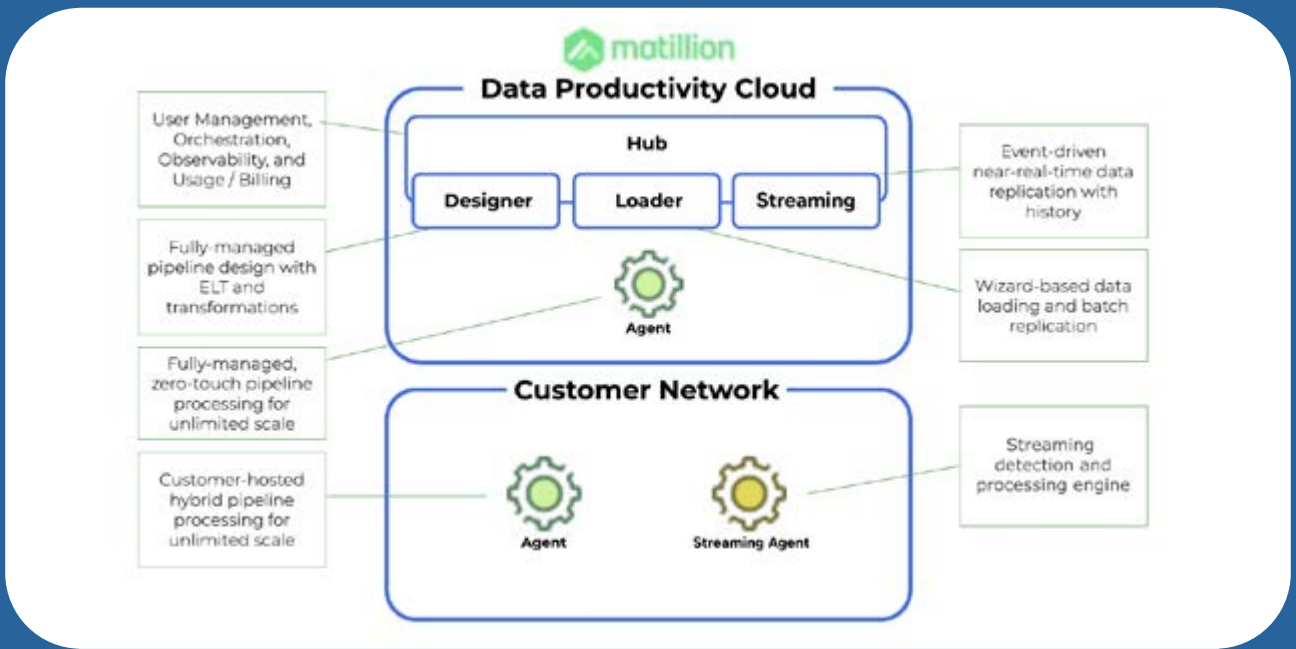
It's important to note that Matillion does not function as a data storage platform. Customer data is not stored within Matillion's systems. Instead, the platform focuses on the orchestration and management of data processes. Any configurations, user information, and metadata stored within the system are encrypted both at rest and in transit, ensuring the highest level of data security.

Matillion Data Productivity Cloud represents Matillion's central solution platform, incorporating a range of applications and components that deliver diverse data services and deployment options. Hosted within Matillion's secure cloud environment, the platform seamlessly integrates with customer networks and virtual networks using standard secure communication protocols. This integration enables efficient and secure data exchange between customer systems and the Matillion platform.

Matillion Data Productivity Cloud leverages the power of advanced data management capabilities, enabling streamlined data processes, enhanced productivity, and timely data insights.

Matillion Data Productivity Cloud comprises applications and services residing inside and outside Matillion's VPC (virtual private cloud), depending on each customer's deployment, and communicating across networks via HTTPS (API microservices). Matillion Data Productivity Cloud is a multi-tenant platform with both logical and physical measures in place to ensure separation. When users log into the Hub they select an account from the list of accounts they have access to. This generates a JWT (JSON Web Token) with a custom claim for the selected account ID.

Matillion Data Productivity Cloud Components



Applications in Matillion Data Productivity Cloud

Hub

Hub serves as the central place for administering and monitoring Matillion Data Productivity Cloud. This web-based application offers a multi-tenant environment, allowing users to access and manage their specific environments and data pipelines efficiently.

One of the key features of Hub is its ability to aggregate metadata from customer environments and data pipelines. This enables real-time visibility and observability into the performance of pipeline runs, as well as any failures that may occur. Providing comprehensive insights into pipeline execution and status empowers Hub users to quickly identify and address any issues, ensuring smooth data processing and minimizing downtime.

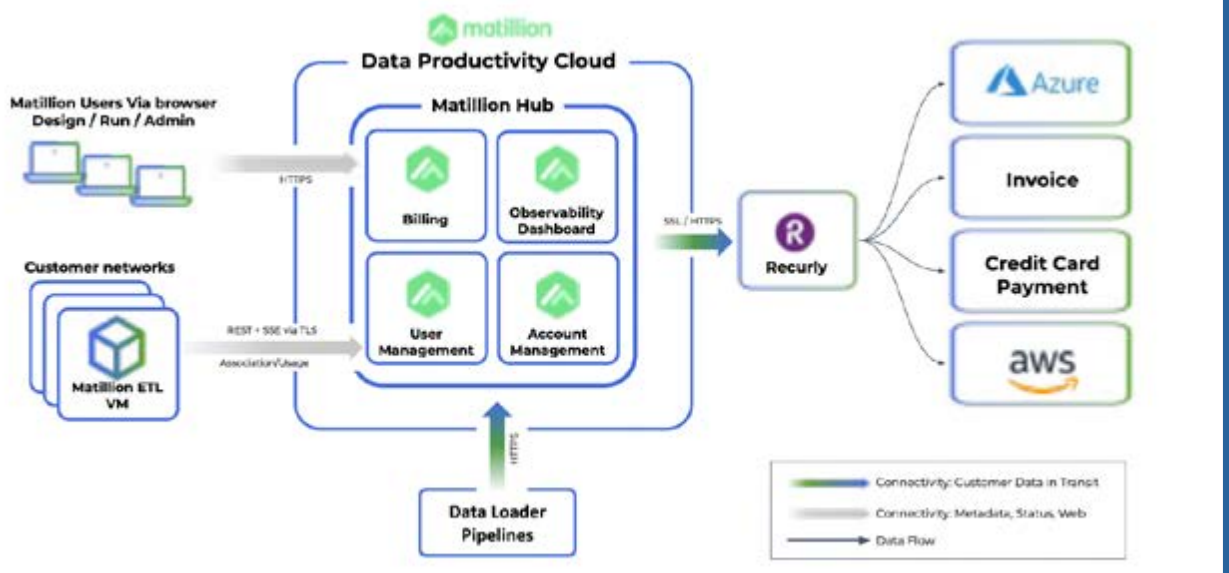
In addition to monitoring pipeline performance, Hub also provides information on credit consumption. This allows users to track and manage their credit usage, ensuring optimal utilization of resources within Matillion Data Productivity Cloud.

Furthermore, Hub offers visibility into the status of Matillion ETL instances. Users can easily monitor the health and availability of their Matillion ETL instances, enabling proactive management and troubleshooting as needed.

The capabilities of Hub allow users to efficiently administer and monitor their data workflows within Matillion Data Productivity Cloud. The centralized nature of Hub enhances operational efficiency, enabling users to gain valuable insights, address issues promptly, and optimize the utilization of their Matillion resources.

Hub does not collect or store customer data, only the data described in the Control Plane section.

Hub Architecture



Designer

Designer is a comprehensive and fully managed data integration pipeline builder. This SaaS web-based application empowers users to create robust and efficient data integration workflows with ease.

As a multi-tenant platform, Designer allows multiple users and teams to work concurrently, leveraging the power of collaborative data integration. With its intuitive interface, users can visually design and configure data pipelines, including data extraction, transformation, and loading processes. The Designer application simplifies complex data integration tasks, enabling users to efficiently handle diverse data sources and formats.

Management, upgrades, and performance of the Matillion control plane are meticulously handled by Matillion's Site Reliability Engineering (SRE) team. This ensures that the control plane remains highly available, reliable, and performs optimally, all while being transparent to our valued customers. With Matillion taking care of the operational aspects, users can focus on designing and implementing their data integration workflows without worrying about infrastructure management.

Designer offers a powerful and streamlined experience for building data integration pipelines. By leveraging its capabilities, users can accelerate their data integration projects, streamline data processes, and unlock the true value of their data assets.

The Designer relies on Agents to connect to data sources and targets using the access credentials provided by the customer, which are stored inside the Matillion Secrets Manager or using OAuth securely at pipeline runtime. The Agent(s) connect to the Hub to retrieve pipelines and schedules, and to provide pipeline execution status for system observability. Agents connect directly to sources and targets, limiting the "hops" of data in transit. Agents leverage the encryption protocols employed by the sources and targets, as configured by users at design time. Transformations are orchestrated inside the cloud data platform target after data is landed (ELT).

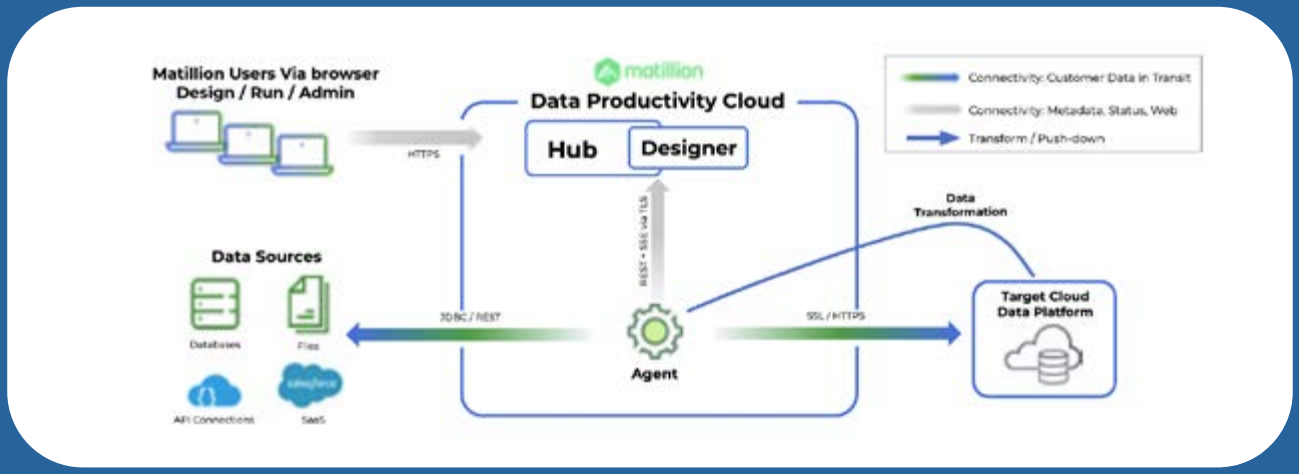
Designer pipelines can operate with two processing models: Matillion-hosted agents, which orchestrate data pipelines from Matillion's control plane, or with customer-hosted Agents in the data plane (inside customers' VPC) to ensure data jurisdiction and isolation requirements are met. These processing models are not mutually exclusive; customers may choose to operate in both modes for different workloads.

Data Sampling

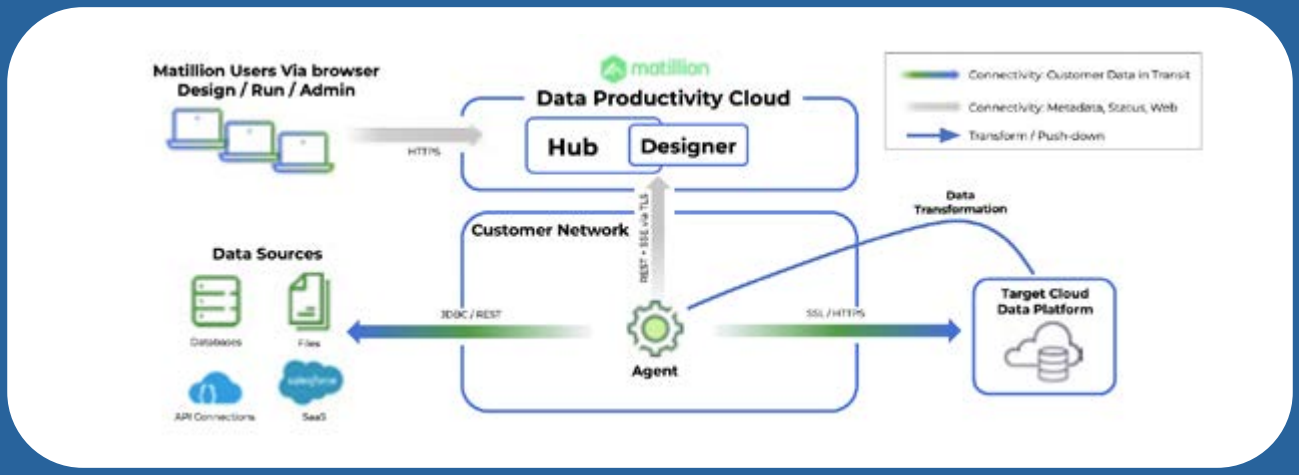
Matillion Data Productivity Cloud includes a design-time sampling capability. Users have the ability to see a sample of data in its post-processing state, should a given component be executed. This is intended to ease the pipeline design process by allowing users to preview the results of pipelines without executing them. The details of this sample data, its flow and protection are:

- In order to perform sampling for a component, a sample request passes through Matillion Data Productivity Cloud to an Agent with access to the customer's data. This Agent may be customer-hosted (running inside the customer's infrastructure) or Matillion-hosted.
- Request from Designer interface: the sample data request specifies how many rows go into the sample based on a user-configured setting, and only this number of rows is subsequently acquired by the Matillion software.
- Once acquired, the sample data passes from the Agent back into Matillion Data Productivity Cloud to reach the design interface.
- The data is not persisted by any service within the platform; for example, no application logs or audits include any sample data.
- Sample data is stored only on the customer (client-side) browser cache and is purged according to customer security policies.
- Sample data is only visible to the user during the local session. Matillion systems do not observe, inspect, or otherwise interact with the sample data.
- Communication between the software agent and Matillion's cloud platform is secured with HTTPS, as is communication between the design interface and the user, guaranteeing customer data is not visible to any third party.

Designer Deployment and Connectivity (Fully Managed)



Designer Deployment and Connectivity (Hybrid)



Agent

The Agent is a key component of the Matillion Data Productivity Cloud. It is responsible for processing pipeline tasks, which are individual units of work within a data integration workflow. These tasks handle data integration and transformation operations by securely connecting to data sources and targets.

By utilizing secure network protocols, the Agent ensures that data is transferred between the Matillion platform and connected data sources in a secure manner. It acts as a bridge, enabling the seamless movement of data while maintaining its integrity and confidentiality.

The Agent can be configured in two ways:

1. In Matillion's cloud network, fully managed by Matillion

2. Inside the customer's cloud virtual network

Matillion Hosted Agent

- The Matillion hosted agent is fully managed by Matillion and resides in Matillion's VPC.
- Connectivity - agents initiate the connection to Matillion's control plane and all communications leverage this outbound pipe
- Agent authentication is performed using OAuth client credentials to ensure access and tenant integrity
- The agents do not need to persist any data - they are designed to be stateless
- Agent health and status information is logged, no customer data is included in these logs
  - Log data is collected by Matillion to enable issues to be investigated and diagnosed
  - Logs cannot be retrieved or removed via the Matillion platform

Customer Hosted Agent

- The customer-hosted agent runs inside the customer's VPC using containerized technologies. Please see Matillion documentation for further information.
- Connectivity - agents initiate connectivity to Matillion's control plane in an outbound manner to get schedules, and exchange the data described below.
  - Agent authentication is performed using OAuth client credentials to ensure access and tenant integrity
  - Agent Instances create an outbound connection to the Matillion Control Plane - no inbound access to the VPC or VNet is required
  - Communication between the Agent and the Control Plane is via HTTPS using TLS 1.2/1.3 encryption
- Data the agent exchanges with the control plane:
  - Agent health & status information including a heartbeat
  - Task run requests
  - Task completion statistics
  - Variable states and values
  - Usage telemetry (no customer data)
- The agents do not persist any data - they are designed to be stateless
  - In the day-to-day execution of pipeline tasks the agents may communicate with the cloud platform's Blob storage and other data services - as needed by the pipeline being executed.
  - The cloud data platform services and assets accessed by the Agent are controlled using the IAM permissions the Agent is assigned.
- Logs are stored by the customer's Container Orchestrator, configured by the customer in their cloud platform.
  - If using the Matillion-recommended ECS Fargate setup, logs are stored within AWS Cloudwatch within the customer's AWS Account, and can be removed from within Cloudwatch. No customer data is stored in these logs.
- Matillion automatically updates customer-hosted agents to ensure you're running the most recent and secure software.

Data Loader

Data Loader is a versatile and user-friendly Software-as-a-Service (SaaS) application designed to facilitate the rapid configuration and execution of batch data load and replication pipelines. With its multi-tenant architecture, multiple customers can leverage the capabilities of Data Loader simultaneously.

The application provides a seamless and intuitive interface for users to configure and orchestrate their data loading and replication workflows. It empowers users to efficiently transfer and synchronize data across various sources and destinations, enabling them to achieve faster data integration and replication processes.

One of the key benefits of Data Loader is that the management, upgrades, and performance tuning of the application are expertly handled by Matillion's Site Reliability Engineering (SRE) team. This ensures that the application remains highly available, performs optimally, and incorporates the latest enhancements and updates. Users can enjoy the benefits of continuous improvements and reliability without any disruption or additional management responsibilities.

With Data Loader, users can simplify and streamline their batch data loading and replication tasks, saving time and effort. By leveraging the power of this SaaS application, users can focus on the data itself and its utilization, while Matillion's SRE team takes care of the operational aspects, ensuring a seamless and efficient experience.

Data Loader is a reliable and efficient solution for managing data loading and replication pipelines, allowing users to accelerate their data integration processes and derive maximum value from their data.

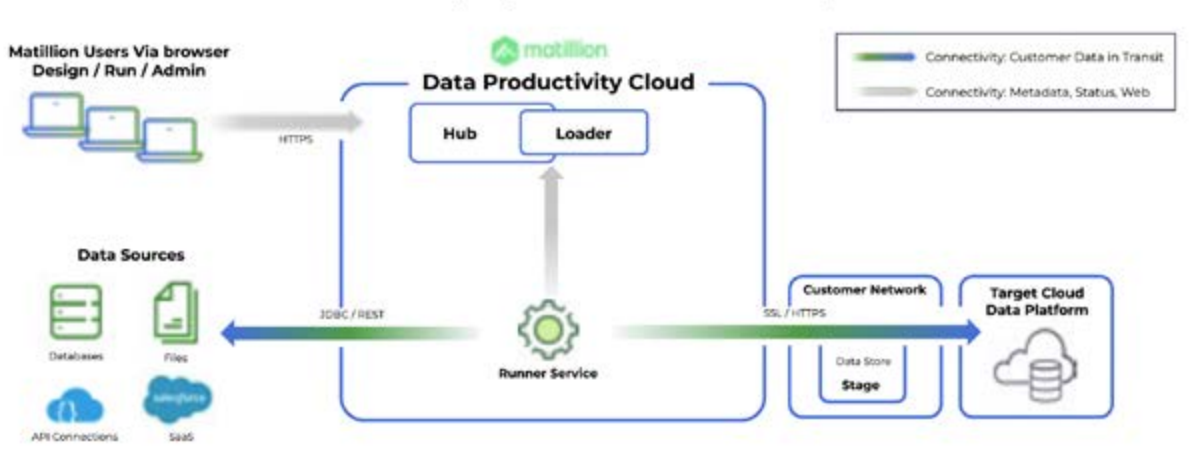
Data Loader pipelines operate with a fully-managed processing model from customer-dedicated virtual resources inside Matillion's control plane.

The Loader connects to data sources and targets using the access credentials provided by the customer, which are stored inside the Matillion Secrets Manager or using OAuth securely at pipeline runtime. The service transmits data using a temporary, isolated runner in the Matillion VPC to pull data from the source and then stages the data to a staging area inside the customer's cloud data platform.

This process leverages the encryption protocols employed by the source service and actively deletes the staged data after loading it into the target data platform. The runner service is non-interactable and is destroyed upon completion of a pipeline.

The runner service then loads the data into the target table in the target data platform; this connectivity is always encrypted via JDBC TLS or HTTPS.

Data Loader Deployment and Connectivity



Data Productivity Cloud Streaming

Data Productivity Cloud Streaming is a powerful and versatile Hybrid Software-as-a-Service (SaaS) application offered by Matillion. It provides customers with a seamless and efficient solution to configure and enable change data capture processes. With its multi-tenant architecture, multiple customers can leverage the capabilities of streaming concurrently.

The application simplifies the configuration and activation of change data capture, allowing users to efficiently capture and track changes made to their data sources in near real-time. By identifying and capturing data modifications, streaming enables users to stay up-to-date with the latest changes in their data, facilitating timely and accurate data integration and replication processes.

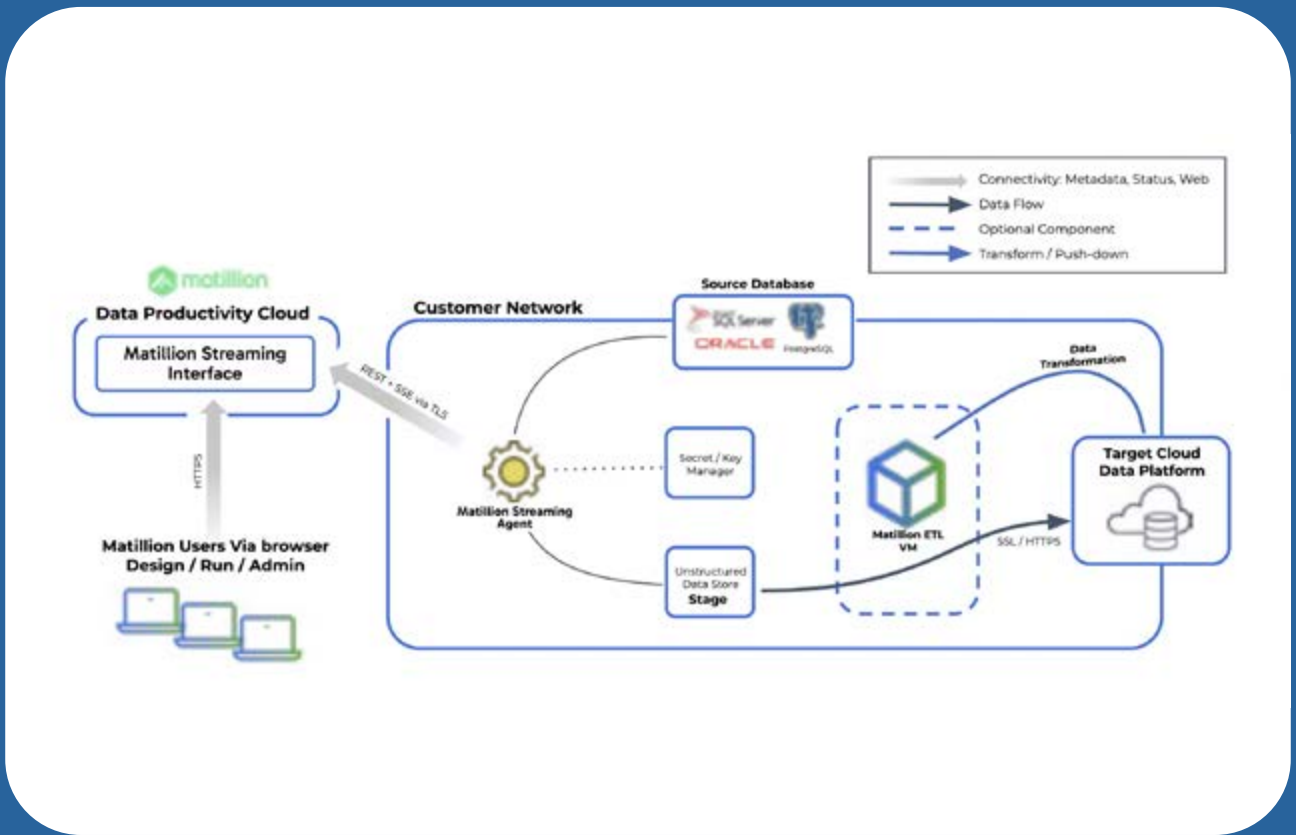
Matillion takes responsibility for the management, upgrades, and performance of the streaming control plane through its dedicated Site Reliability Engineering (SRE) team. This ensures that the control plane remains highly available, performs optimally, and incorporates the latest enhancements and updates.

With Streaming, customers leverage the captured changes for various use cases, such as data synchronization, data integration, and real-time analytics. The application streamlines the process of capturing and managing changes, providing users with the flexibility and agility needed to respond quickly to evolving data requirements.

Matillion Streaming is a reliable and efficient solution that empowers users to configure and enable change data capture processes with ease. Matillion Streaming enables customers to accelerate their data integration workflows and stay synchronized with the latest changes in their data sources, unlocking the full potential of their data.

Streaming pipelines are processed by Streaming Agents, which are configured from the Streaming web UI but reside in the customer's data plane.

Data Productivity Cloud Streaming Deployment and Connectivity



Updates and Version Control for Matillion Data Productivity Cloud platform

The Matillion Data Productivity Cloud platform undergoes a meticulous process for updates and version control, ensuring the stability and reliability of the platform. Each release goes through three distinct environments, each with specific quality assurance measures applied.

The first environment is a development environment where new features and enhancements are implemented and tested. Here, the development team ensures that the changes meet the required specifications and standards.

Once the development phase is complete, the release moves to a testing environment. In this environment, comprehensive testing procedures are conducted to validate the functionality and performance of the new release. This includes various types of testing, such as functional testing, integration testing, and regression testing, to identify and address any issues or conflicts.

After successful testing, the release progresses to a staging environment. Here, it undergoes further verification and validation to ensure that it is ready for deployment to the production environment. This includes performance testing, security checks, and user acceptance testing, among others.

Promotions to the production environment are performed by a limited number of authorized Site Reliability Engineers, adhering to the principle of least privilege. This strict access control ensures that only qualified personnel can perform deployments to the live production environment.

To maintain a high level of security and accountability, all access to these environments is logged and monitored using Matillion's security monitoring and alerting system. This allows for comprehensive tracking and analysis of all activities within the environments, enhancing the platform's overall security posture.

Following this rigorous update and version control process ensures that the Matillion Data Productivity Cloud platform remains stable, reliable, and secure, providing customers with a robust and trustworthy solution for their data integration needs.

Matillion Data Productivity Cloud Control Plane Security

Security is a top priority for the Matillion Data Productivity Cloud, and its control plane is designed with robust measures to ensure the confidentiality, integrity, and availability of customer data and the platform itself.

One key aspect of control plane security is the strict separation of components, configurations, and networks. Matillion Data Productivity Cloud's control plane is entirely segregated from all other Matillion assets, preventing unauthorized access and reducing the risk of potential vulnerabilities.

Access to the control plane is governed by the principle of least privilege, which means that only authorized personnel with a legitimate need can access the system. This approach ensures that access rights are granted on a "need-to-know" basis, minimizing the potential for unauthorized actions or data breaches.

Furthermore, Matillion implements rigorous access controls and authentication mechanisms to verify the identity of users accessing the control plane. This includes robust authentication protocols, such as multi-factor authentication, to strengthen the security of user accounts and prevent unauthorized access.

Access to Matillion production systems is strictly controlled via our access control infrastructure. We have established a 'break-glass' process that is documented and auditable in case emergency access is needed for incident mitigation. Access is removed automatically upon conclusion of such an the incident.

Matillion employs industry best practices for securing the control plane's network infrastructure, including firewalls, network segmentation, and intrusion detection and prevention systems; measures which help protect against unauthorized network access and mitigate the risk of network-based attacks.

Regular security assessments and audits are conducted to evaluate the effectiveness of control plane security controls and identify any potential vulnerabilities. This allows Matillion to proactively address security risks and ensure that the control plane remains resilient against emerging threats.

Implementing these stringent security measures, including component separation, access control, authentication mechanisms, network security, and regular assessments allows Matillion to safeguard Matillion Data Productivity Cloud's control plane and provide customers with a secure and trustworthy platform for their data integration needs.

Authentication and User Access

Matillion understands the importance of aligning customer authentication needs with enterprise requirements. To cater to this, we offer multiple options for user authentication in Matillion Data Productivity Cloud. Our goal is to provide a secure and flexible access control solution that meets organizations' specific needs.

Unified Login and User Administration:

Our platform enables unified login and user administration on a per-tenant basis. This means that customers have full control over user access and can configure it according to their preferences. Choose between standard user/password authentication or opt for more advanced options such as token-based Single Sign-on (SSO) and Multi-Factor Authentication (MFA). This ensures that only authorized users can access the Matillion environment.

Role-Based Access:

We recognize the importance of separating duties and enforcing the rule of least privilege within an organization and as such, our platform supports role-based access control. Customers can configure roles for different functions and assign appropriate privileges to each role. This ensures that users have access only to the functionalities and data they require to perform their specific tasks.

SSO and Centralized User Management:

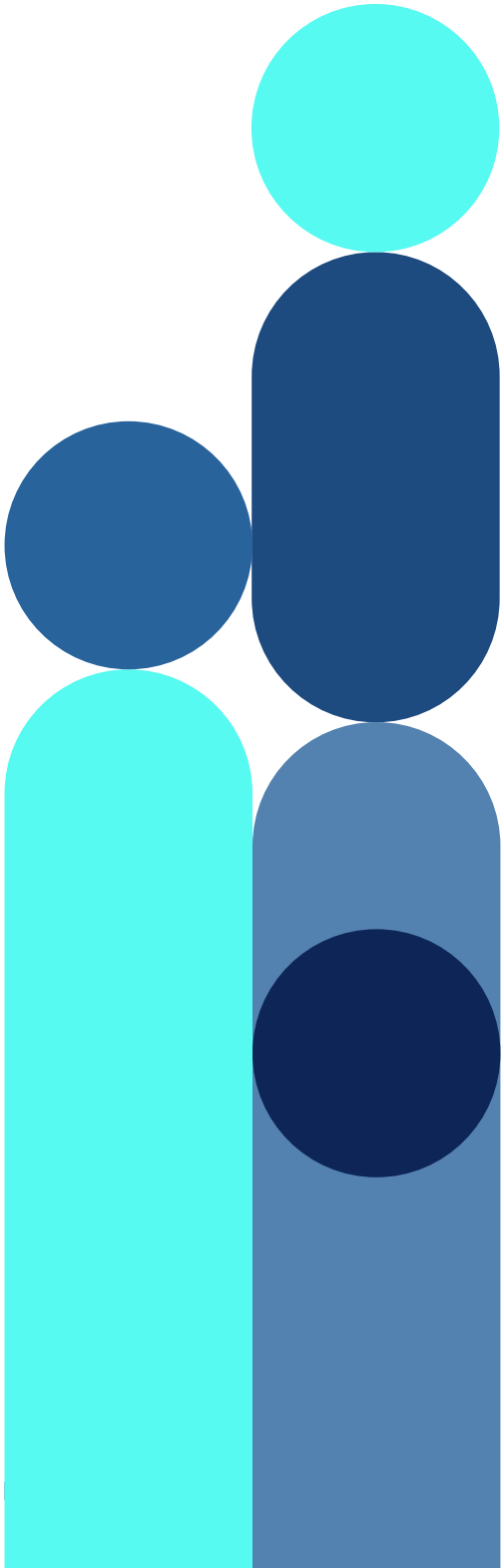
To streamline the authentication and authorization process, Matillion Data Productivity Cloud leverages Single Sign-on (SSO). With SSO, customers' existing identity provider can be used to manage user access across multiple Matillion applications. This centralized user management approach simplifies the administration process and ensures consistency in authentication and authorization practices.

We provide a secure and user-friendly authentication experience for our customers. Offering a range of authentication options, role-based access control, and leveraging SSO for centralized user management, Matillion Data Productivity Cloud ensures that organizations' authentication needs are met effectively and in line with industry best practices.

Matillion Data Productivity Cloud Shared Responsibility

Matillion follows a shared responsibility model, which outlines the responsibilities of both Matillion as the cloud service provider and our customers when it comes to securing data and applications in the cloud. This collaborative approach ensures that data and systems hosted in Matillion Data Productivity Cloud are protected effectively and that both parties play an active role in maintaining a secure environment.

The shared responsibility model consists of three planes: the control plane, the Matillion data plane, and the customer data plane.



Control Plane:
The control plane is managed by Matillion and encompasses the infrastructure, network, and services that power Matillion Data Productivity Cloud. Matillion takes responsibility for the security of the underlying infrastructure, including physical security, network security, and platform-level security controls. We ensure that the control plane is resilient, available, and protected against external threats.

Matillion Data Plane:
The Matillion Data Plane includes the components and services provided by Matillion within Matillion Data Productivity Cloud. Matillion is responsible for securing and maintaining these components, including the Hub, Designer, Agents, and other Matillion-managed services. We apply industry best practices to ensure the security and integrity of these components, including regular updates, patches, and vulnerability management.

Customer Data Plane:
The customer data plane refers to the data and applications that customers upload, process, and store within Matillion Data Productivity Cloud. Customers have the primary responsibility for securing their data, defining access controls, and implementing appropriate security measures. This includes configuring user access, managing authentication, and applying data encryption or obfuscation as necessary. Matillion provides the necessary tools and features to enable customers to secure their data effectively within Matillion Data Productivity Cloud.

Our shared responsibility model ensures that both Matillion and our customers work together to create a secure cloud environment by clearly defining the responsibilities in each plane. Matillion takes care of the underlying infrastructure and platform security, while customers maintain control over their data and implement necessary security measures within their applications.

It is important for customers to understand and fulfill their obligations within the shared responsibility model, as this collaboration is essential for maintaining a secure and reliable cloud environment for all users of Matillion Data Productivity Cloud.

Perimeter Security for Matillion Data Productivity Cloud

The security of Matillion Data Productivity Cloud perimeter is a top priority for Matillion. To protect against potential threats and unauthorized access, we employ a range of standard security measures that safeguard the perimeter surface area.
These measures include:

- **Web Application Firewall (WAF):**
  A Web Application Firewall is deployed to monitor and filter incoming web traffic to Matillion Data Productivity Cloud. It helps detect and block malicious activities, such as cross-site scripting (XSS) attacks, SQL injection, and other web application vulnerabilities.

- **Distributed Denial of Service (DDoS) Attack Protection:**
  To mitigate the risk of DDoS attacks, we have implemented robust DDoS protection mechanisms. These mechanisms detect and mitigate large-scale volumetric attacks, ensuring the availability and performance of Matillion Data Productivity Cloud.

- **Network-based Intrusion Detection System (IDS):**
  An Intrusion Detection System is in place to monitor network traffic and identify any suspicious or potentially malicious activities. The IDS analyzes network packets, looking for patterns and signatures associated with known threats or attack vectors. Upon detection, appropriate actions are taken to address the identified threats.

- **Network-based Intrusion Prevention System (IPS):**
  In addition to the IDS, we utilize an Intrusion Prevention System to actively block and prevent identified threats from compromising Matillion Data Productivity Cloud. The IPS operates in real-time and automatically responds to potential threats by applying predefined security rules and policies.

- **Cloud Security Posture Management (CPSM):**
  To maintain a secure configuration and compliance posture, Matillion employs Cloud Security Posture Management solutions. These tools continuously monitor Matillion Data Productivity Cloud environment, identify misconfigurations, and provide recommendations to ensure compliance with security best practices and industry standards.

These standard security measures work in combination to provide comprehensive protection for Matillion Data Productivity Cloud perimeter. Matillion is committed to maintaining the highest level of security and employs these measures to safeguard customer data, applications, and the overall integrity of the cloud environment.

It is worth noting that these perimeter security measures are just one aspect of Matillion's comprehensive security program. We implement multiple layers of security controls and follow industry best practices to ensure the overall security and protection of Matillion Data Productivity Cloud.

Customer Data Retention Policy

In Matillion Data Productivity Cloud, the control plane databases store various types of customer data. The retention rules for these data vary based on the type of data being stored. It's important to note that the residency of the control plane is determined by the customer's selection of the Matillion resident data center, which can be in North America or in the EU.

Matillion follows secure and compliant practices to ensure the storage and retention of customer data. Here are some key points regarding data storage and retention in the Matillion control plane:

- **Data Types:**
  The control plane databases store different types of customer data, including configurations, user information, and metadata. These data elements are necessary for managing and operating Matillion Data Productivity Cloud.

- **Data Residency:**
  Matillion offers customers the choice to select the data center location that aligns with their requirements. This ensures that the control plane and the stored customer data are hosted within the customer's chosen region, either in North America or in the EU.

- **Data Retention:**
  The retention rules for customer data in the control plane are determined based on the type of data stored. Matillion follows appropriate data retention practices and complies with applicable data protection regulations. The specific retention periods may vary depending on factors such as data classification, legal requirements, and business needs.

- **Data Security:**
  Matillion takes data security seriously and employs robust measures to protect the confidentiality, integrity, and availability of customer data. Encryption is applied to data at rest and in transit.

- **Compliance:**
  Matillion adheres to relevant data protection and privacy regulations, such as the General Data Protection Regulation (GDPR), and other applicable regional laws. By following these regulations, Matillion ensures that customer data is handled and retained in a manner that respects privacy and compliance requirements.

Matillion maintains a strong commitment to data security and privacy. By securely storing customer data in the control plane databases and adhering to appropriate retention rules, Matillion provides a reliable and trusted environment for customers to manage their data integration processes effectively.

Customer Data Types

The following table outlines the different types of customer data collected and processed by Matillion:

Data Type	Description
Account / Billing Data	Customer's billing information, including invoices, receipts, and payment details.
Telemetry Data	Data generated by customers' usage of your software /application, such as logs, performance metrics, and error reports.
Customer Created Pipelines / Code	Code, scripts, or any custom jobs created by customers on our platform.
Support Cases	Information related to customer support inquiries, including tickets, emails, and chat logs.
Customer Data Source & TargetKeys and Credentials	Secrets used by pipelines to access customer data, retrieved at pipeline runtime.

Data Retention Policy

The following table outlines the data retention policy for each customer data type:

Data Type	Retention Period	Purpose
Account / Billing Data	7 years	Comply with financial and accounting regulations, track payment history, and address billing inquiries.
Telemetry Data	7 years	Analyze software/application performance, troubleshoot issues, and improve the product/service.
Support Cases	3 years	Maintain a record of customer inquiries, track issue resolution, and improve customer support services.

Encryption at rest

- Metadata stored in the Matillion control plane is encrypted at the volume level, using a 256-bit AES-GCM encryption key (stored in KMS).
- All customer secrets, including data source/target credentials used in Matillion pipelines, are persisted into a HashiCorp secrets vault. The vault uses process authentication and tenancy boundaries to allow Agents executing customer workloads to access the appropriate credentials at pipeline runtime (including design-time pipeline creation). Credentials are encrypted at every step via HashiCorp standards, and they are not persisted and not retrievable.

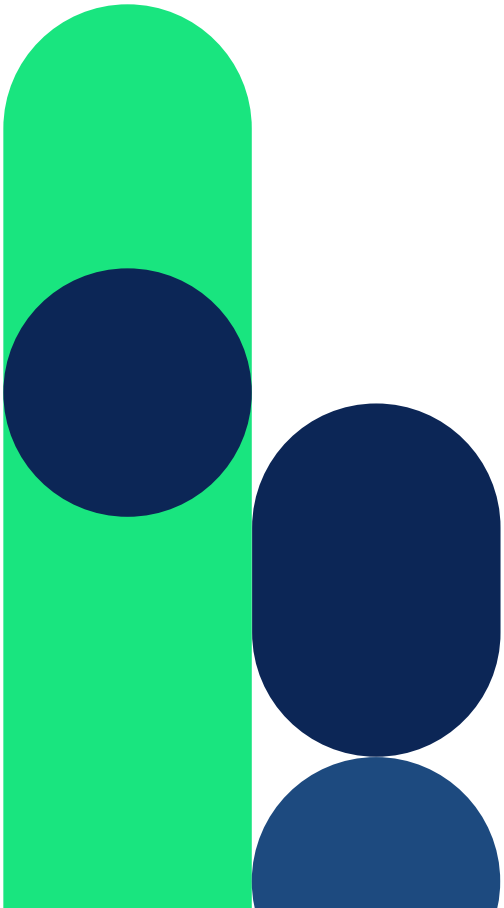
Data Destruction and Security

At the end of the specified retention periods, all customer data will be securely deleted or anonymized unless a legal obligation requires its further retention. Data destruction will be performed in compliance with industry best practices and applicable regulations to prevent unauthorized access or disclosure.

Matillion implements appropriate security measures to protect customer data throughout its retention period.

Legal and Regulatory Compliance

This data retention policy is subject to applicable laws and regulations governing data privacy, security, and protection. Matillion regularly reviews and updates the policy to ensure compliance with evolving legal requirements.



SaaS Availability and Redundancy

Matillion Data Productivity Cloud is designed to be fully redundant and highly available, ensuring continuous access and reliability for customers. The cloud platform consists of two categories of services: Core services and Application services, each offering different levels of redundancy.

01

Core Services:

Core services form the foundational components of the Matillion Data Productivity Cloud architecture. These services are designed with Active-Active redundancy, meaning they are replicated and synchronized across primary and secondary regions, each comprising a minimum of three availability zones. This redundancy ensures that in the event of an outage or failure in one region, services remain accessible and operational in the other. The core services maintain the following Recovery Point Objective (RPO) and Recovery Time Objective (RTO):

- RPO: 3 hours (maximum acceptable data loss)
- RTO: 12 hours (maximum acceptable downtime)

02

Application Services:

Application services within Matillion Data Productivity Cloud deliver specific features and functionality to customers. These services also maintain a high level of availability through regional redundancy. Similar to core services, application services are distributed across multiple availability zones within a region. This redundancy provides resilience and ensures that services remain accessible even in the face of localized failures. The application services maintain the following RPO and RTO:

- RPO: 12 hours (maximum acceptable data loss)
- RTO: 24 hours (maximum acceptable downtime)

Matillion implements this model of redundancy and availability to provide high assurance to customers regarding the availability and accessibility of their configurations, accounts, users, metadata, and other important data stored within Matillion Data Productivity Cloud.

It's important to note that these RPO and RTO values represent the maximum acceptable limits for data loss and downtime, and Matillion continuously works to minimize these values through robust infrastructure and operational practices. The goal is to ensure that customers can rely on the platform for their data integration needs without disruptions or data loss.

Matillion ETL

Matillion ETL is an enterprise cloud data integration product that offers customers flexibility and control over their deployment. It is deployed as a virtual machine (VM) image within a customer's Virtual Private Cloud (VPC). As a hosted web application, it enables customers to process data pipelines at scale, with the sizing and resources configured based on the customer's requirements.

This deployment methodology offers customers the scalability and flexibility of cloud-based data integration and the control and customization capabilities associated with self-hosted applications, allowing customers to align with their specific networking and monitoring requirements.

Because Matillion ETL is deployed inside the customer's cloud network, no customer data is transferred between the Matillion Virtual Private Cloud (VPC) and the customer network.

Updates and Version Control for Matillion ETL

Matillion ETL follows a structured process for updates and version control to ensure customers have access to the latest features, bug fixes, and security updates. The updates are delivered directly from source control repositories maintained by Matillion.

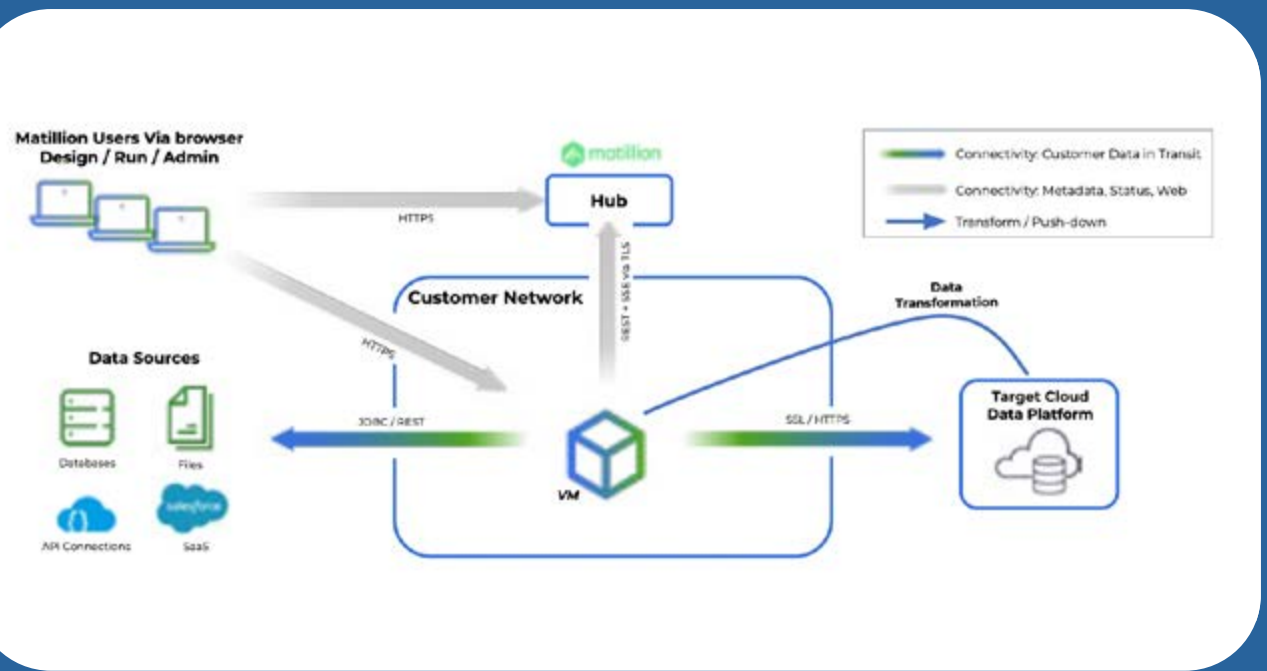
Typically, major releases of Matillion ETL are pushed to the repositories approximately every eight weeks. These major releases introduce new features, enhancements, and improvements to the product. However, for critical bug fixes and security updates, incremental releases and hotfixes may be published more frequently as needed to address specific issues.

When it comes to updating Matillion ETL deployed within a customer's Virtual Private Cloud (VPC), customers have the flexibility to choose when to apply the updates. This allows customers to control the timing and impact of updates on their environment, taking into consideration any dependencies or specific requirements they may have.

To learn more about updating Matillion ETL and the recommended update procedures, please refer to the documentation, offering detailed instructions and guidelines to help customers successfully update their Matillion ETL instances while minimizing any potential disruptions.

By regularly updating Matillion ETL, customers can take advantage of new features, performance enhancements, and security patches, ensuring they have access to the latest capabilities and maintaining the integrity and security of their data integration processes.

Matillion ETL Deployment and Connectivity



Application Security Features

Matillion prioritizes application security and offers various features to ensure compatibility with complex enterprise architectures. Some of the key application security features provided by Matillion ETL are:

Signed Certificates for HTTPS Connections: Matillion ETL supports the use of signed certificates for secure HTTPS connections, ensuring encrypted communication between Matillion ETL and client applications.

TLS 1.2+ for Data Source and Target Connections: Matillion ETL uses Transport Layer Security (TLS) version 1.2 or higher for secure data source and target connections. TLS encrypts the data transmitted between Matillion ETL and external systems, safeguarding it from unauthorized access.

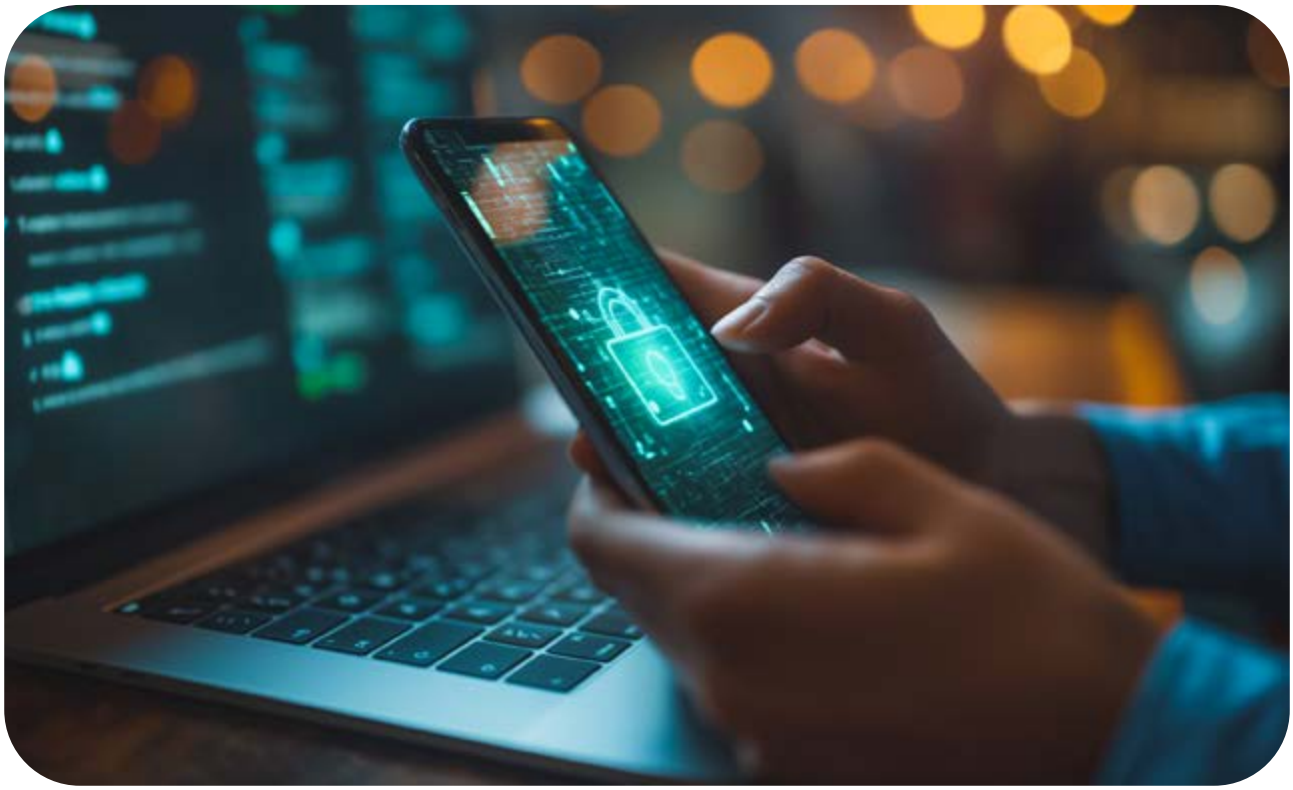
KMS Encrypted Secret Stores: Matillion ETL incorporates Key Management Service (KMS) encrypted secret stores, which allow secure storage and management of sensitive information such as credentials, API keys, and other secrets. Encryption ensures that the secrets are protected even if unauthorized access to the storage occurs.

Multiple Levels of Authorization: Matillion ETL provides multiple levels of authorization to control access to different functionalities and resources within the platform. This enables organizations to enforce the principle of least privilege, ensuring that users have only the necessary permissions to perform their tasks.

OAuth Connectivity Components for Data Sources: Matillion ETL supports OAuth connectivity components, enabling secure and authenticated access to various data sources that utilize OAuth for authorization. This feature enhances the security of data integration processes by leveraging industry-standard authentication mechanisms.

Integration with OpenID Connectors for Authentication: Matillion ETL offers integration with OpenID connectors, allowing customers to leverage OpenID Connect for user authentication. OpenID Connect is an identity layer on top of OAuth 2.0, providing secure and standardized authentication for web and mobile applications.

These application security features ensure Matillion can provide customers with a secure and reliable platform that can seamlessly integrate into their existing enterprise architectures to safeguard sensitive data, establish secure connections, and ensure proper authentication and authorization mechanisms are in place.



Data Productivity Cloud AI FAQs

What do Matillion's AI features do?

Matillion incorporates pipeline components that allow customers to enrich their data, using third-party LLMs ("AI in the pipeline"). Additionally, Matillion provides productivity features with AI, such as auto-documentation and AI Copilot, which helps to build pipelines using natural language ("AI in the product").

What AI capabilities are available in Matillion Data Productivity Cloud?

- AI in the product - Using the AI to improve the user experience in the product, bring more intelligence when designing/operating/monitoring pipelines, automate gestures, help troubleshoot, and generally improve productivity
- AI in the data pipelines - Use AI to augment and enrich customer data

Does Matillion provide its own AI processing capabilities for the AI Prompt components?

No. Matillion leverages the customer's 3rd-party services (including, but not limited to, AWS BedRock or OpenAI ChatGPT) as subprocessors, and by using Matillion AI features, a customer consents to Matillion's use of subprocessors.

Does Matillion use my data to train third-party AI models?

No. Your data isn't used to train models or refine our AI service. Matillion AI auto-documentation solely relies on prompt engineering to translate Data Pipeline Language (DPL) into business literacy.

In some cases, Matillion AI is trained on metadata (i.e. DPL prompts) and internal data (i.e. DPL pipelines, product documentation, data engineering best practices, and technical metadata) to generate pipelines. There's no customer data involved, and there's no reinforcement learning process based on your data. Our internal Matillion AI service doesn't and cannot view customer data.

Can customers bring their own AI accounts?

Yes. Customers integrate with AI Large Language Models via the AI Prompt component setup, using the API Key from their GenAI provider. Matillion doesn't provide a built-in AI provider for the AI Prompt components.

Can customers opt out of Matillion's AI features?

Yes. Customer consent is required to use AI and Matillion allows customers to disable the AI features if they have concerns.

How is my data protected when using AI features?

Matillion does not persist AI-generated data within our systems. Passwords and secrets aren't sent to the AI service and are only resolved at pipeline runtime by a secure service. All data is encrypted in transit as documented in Matillion's security whitepaper.

What is Matillion's commitment to responsible AI use?

At Matillion, our goal is to enhance human productivity, not replace it. We believe in harnessing AI to empower you and your teams for greater success.

Where can I find more information about Matillion's security architecture and processes?

Please visit **trust.matillion.com** for further information.

Summary

Matillion is a trusted leader in secure cloud data management. We prioritize the security of our systems through a comprehensive, standards-based security framework covering infrastructure, network, data privacy, access control, incident response, and software development. Matillion complies with all common privacy standards, including GDPR and CCPA, to ensure personal data protection. Matillion products offer secure and scalable data movement, transformation, orchestration, and observability. We leverage a shared responsibility model, provide robust authentication options, and maintain high availability.

For more information, contact **sales@matillion.com**